IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA,

Plaintiff,

v.

680,467.92 TETHER (USDT) VIRTUAL
CURRENCY SEIZED FROM OKX
ACCOUNT USER ID 422338420543782467,

and

480.996 BINANCE COIN (BNB) VIRTUAL
CURRENCY SEIZED FROM OKX
ACCOUNT USER ID 438957971071216816,

Defendants *in Rem*.

Civil No. 1:24-cv-1065

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

COMES NOW the plaintiff, the United States of America, by and through its counsel, Jessica D. Aber, United States Attorney for the Eastern District of Virginia, and Kevin Hudson, Assistant United States Attorney, and brings this complaint and alleges as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

NATURE OF THE ACTION

1. The United States brings this action *in rem* seeking the forfeiture of all right, title, and interest in the defendants *in rem* identified in the case caption above (together, the "Defendant Property").

2. The United States' claim arises from wire fraud, money laundering violations, the carrying on of unlawful activity as that term is defined under 18 U.S.C. § 1952(b), and computer fraud.

3. The Defendant Property constitutes the proceeds of violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1952 (use of facilities in interstate/foreign commerce to carry on unlawful activity), and 18 U.S.C. § 1030 (fraud in connection with computers). In addition, the Defendant Property is property involved in transactions in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering). The Defendant Property is therefore subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 981(a)(1)(A).

THE DEFENDANTS *IN REM*

4. Defendant 480.996 Binance Coin virtual currency ("BNB") was seized from OKX account user ID 438957971071216816 and is currently held in a cryptocurrency wallet controlled by the Federal Bureau of Investigation ("FBI") in the Eastern District of Virginia.[1]

5. Defendant 680,467.92 Tether virtual currency ("USDT") was seized from OKX account user ID 422338420543782467 and is currently held in a cryptocurrency wallet controlled by the FBI in the Eastern District of Virginia.[2]

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over actions commenced by the United States under 28 U.S.C. § 1345, and over forfeiture actions under 28 U.S.C. § 1355(a) and (b).

7. This Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. § 1355(b)(1)(B) because the Defendant Property is located in the Eastern District of Virginia and

[1] Of the total amount of BNB referenced in Paragraph 4, 10 BNB was seized by law enforcement on June 8, 2023, and the remaining 470.996 BNB was seized on June 9, 2023.

[2] Of the total amount of USDT referenced in Paragraph 5, 100 USDT was seized by law enforcement on June 13, 2023, and the remaining 680,367.92 was seized on June 16, 2023.

because certain acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia.

8. Venue is proper within this judicial district under 28 U.S.C. § 1355(b)(1)(B) because the Defendant Property is located in the Eastern District of Virginia and because certain acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia.

FACTUAL ALLEGATIONS

Background

The SafeMoon Cryptocurrency Token

9. SafeMoon, LLC ("SafeMoon") is a Utah-headquartered cryptocurrency and blockchain company that created the SafeMoon cryptocurrency token ("SFM").

10. SFM is a decentralized finance ("DeFi") token, which means that it operates without the need for a traditional, centralized intermediary, such as a bank or broker.

11. The fact that SFM is a cryptocurrency *token*, as opposed to a cryptocurrency *coin*, is not a purely academic matter: cryptocurrency tokens operate on an already-existing blockchain, whereas cryptocurrency coins operate on their own blockchain.

12. SFM operates on the Build N Build Chain blockchain network (the "BNB Chain").

13. The BNB Chain supports the use of smart contracts, which are essentially digital contracts that are automatically executed when predetermined conditions are met.

14. SafeMoon uses smart contracts to manage the creation, supply, and liquidity of SFM.

15. To facilitate the liquidity of SFM, SafeMoon uses a smart contract to secure a digital supply of cryptocurrency assets in an entity known as a liquidity pool.

16. Liquidity pools are designed to ensure that there is always a sufficient amount of liquidity in the market, which – in theory – should prevent large fluctuations in the price of the cryptocurrency.

17. The SFM liquidity pool holds a reserve of SFM and an equivalent value of BNB.

18. Notably, the servers on which the SFM liquidity pool operate are connected to the Internet, and users throughout the world trade SFM.

The BNB Chain

19. The BNB Chain is a decentralized blockchain ecosystem that allows users to transact safely without having to rely on third parties.

20. In its simplest terms, a blockchain is a distributed database or ledger that maintains a continuously growing list of ordered transactional records, known as blocks, that are linked together via cryptography.

21. A blockchain transaction involving cryptocurrency is not necessarily a financial transaction in a traditional sense, but rather, it is an instruction submitted by a user to reallocate something from one address to another.

22. For example, a transaction could involve an instruction to reduce the amount of a certain cryptocurrency in one account and to add the same amount to another account.

23. The “transaction” occurs when the data on the blockchain is updated to reflect a debit from one account balance and a credit to the other account balance.

24. The BNB Chain, like other decentralized blockchain platforms, relies on validators to process and confirm transactions on the network and add them to the blockchain.

25. When a transaction is initially submitted on the BNB Chain, it remains pending in a local memory pool, or “mempool” for short, until it is picked up by a validator.

26. Users must pay certain fees in order to execute a transaction on the BNB Chain, to include a "gas fee" that is used to pay validators for the resources needed to process and confirm the transaction.

27. Given that validators have the power to determine the order in which transactions are processed, a user can elect to pay a higher gas fee when submitting a transaction as a way to incentivize the validators to prioritize the transaction.

28. Conversely, if a user offers too little in gas fees, the transaction may be executed late or not at all.

29. Simply put, the more a user is willing to pay in gas fees, the faster the transaction will be processed.

30. And once a transaction is processed and confirmed, it is included in a block and removed from the mempool.

Crypto-Trading Robots and Frontrunning

31. The use of automated crypto-trading robots, or "bots" for short, has become an increasingly popular tool for cryptocurrency traders.

32. A bot is an automated software program that executes trades on behalf of a user using pre-defined strategies and/or pre-determined parameters with the aim of generating profits.

33. A frontrunning bot is a type of bot programmed to take advantage of the latency in a blockchain network by executing profitable trades ahead of others.

34. Frontrunning bots scan pending transactions submitted to the public mempool and simulate those transactions to determine their profitability.

35. For the transactions that a frontrunning bot deems sufficiently profitable based on pre-programmed criteria, the bot will create a transaction that in essence duplicates the pending

transaction and offers a higher gas fee to ensure that its transaction will be prioritized ahead of the transaction it duplicated.

36. Ultimately, the users of frontrunning bots seek to enrich themselves by mimicking pending trades submitted by other traders in order to capture the profits that those other traders would have made.

The Scheme to Defraud SafeMoon

37. In March 2023, an unidentified exploiter (the "Exploiter") devised and intended to devise a scheme to defraud SafeMoon and to deprive SafeMoon of money and property by means of fraudulent pretenses.

38. The key piece of the Exploiter's scheme involved the exploitation of a vulnerability in a recently updated SFM smart contract.

39. More specifically – and within hours of the update to the SFM smart contract at issue – the Exploiter identified that the smart contract included a "burn function" that was mistakenly set to public without restrictions, which allowed any user from any address to remove or "burn" SFM tokens from the SFM liquidity pool.

40. It was part of the Exploiter's scheme to cause the burning of a large amount of SFM tokens held in the liquidity pool using the burn function, which, in turn, would cause the price of SFM to artificially spike.

41. It was further part of the Exploiter's scheme to cause the sale of previously purchased SFM at the fraudulently manipulated price immediately following the execution of the burn function.

42. In simple terms, the sale of SFM at an artificially inflated price would cause a loss to SafeMoon because the seller would be able to withdraw more BNB from the SFM liquidity pool than he or she would otherwise be able to at a non-manipulated price.

43. The Exploiter's scheme was designed to obtain BNB from the SFM liquidity pool under fraudulent pretenses and cause a substantial loss to SafeMoon.

The Transaction

44. On March 28, 2023, at 07:26 UTC, the Exploiter initiated an illicit transaction utilizing a smart contract on the BNB Chain network, which involved a sequence of instructions to: first, purchase a certain amount of SFM tokens at market price; second, execute the public burn function to burn most of the SFM tokens in the SFM liquidity pool; and third, sell the initially purchased SFM back to the liquidity pool immediately following the burn.

45. While the Exploiter's transaction was pending in the public mempool, however, a front-running bot (the "Bot") most likely programmed by a different user (the "Bot User") accessed and evaluated the Exploiter's illicit transaction and determined that the transaction was sufficiently profitable based on its pre-programmed criteria.

46. The Bot executed a smart contract that essentially duplicated the Exploiter's illicit transaction, offering higher gas fees and directing the profits from the transaction to an account controlled by the Bot User.

47. Given the higher gas fees, the BNB Chain validators processed and confirmed the Bot's transaction first, which caused the Exploiter's transaction to fail.

48. Nevertheless, the transaction succeeded in causing the price of SFM to artificially spike, and 27,388 BNB – valued at over $8.5 million on the day of the transaction – was

ultimately withdrawn from the SFM liquidity pool and sent to the Bot's virtual address 0x286E09932B8D096cbA3423d12965042736b8F850.

49. Thereafter, the Bot User subsequently forwarded the funds to the virtual address 0x237D58596F72C752a6565858589348D0fCe622ed ("0x237D").

50. The Bot would not have been able to execute the transaction without the Exploiter's transaction already existing in the mempool.

The Bot User's Subsequent Extortion

51. Within a few hours of the illicit transaction, the Bot User posted a message on the BNB Chain directed to SafeMoon that stated: "Hey relax, we are accidently frontrun an attack against you, we would like to return the fund, setup secure communication channel, lets talk."

52. Thereafter, the Bot User engaged in on-chain and off-chain messaging with SafeMoon.

53. Instead of working with SafeMoon to return the funds, however, the Bot User either explicitly or implicitly threatened to withhold the entirety of the funds that rightfully belonged SafeMoon if SafeMoon did not agree to allow the Bot User to keep a certain percentage of the funds as a bounty for, in the Bot User's own words, its "accidental[] frontrun."

54. The Bot User's threat caused SafeMoon to acquiesce to the Bot User's demand to keep 20% of the proceeds.

55. In other words, the Bot User's threat caused SafeMoon to part with property that was rightfully its own.

56. By April 20, 2023, the Bot User sent 21,904 BNB (80% of the proceeds obtained from the illicit transaction) from 0x237D to a SafeMoon-controlled address.

57. The remaining 20% of the proceeds – approximately 5,476 BNB – were in fact retained by the Bot User.

The Bot User’s Subsequent Money Laundering

58. Despite knowing that the funds the Bot User obtained represented the proceeds of some form of unlawful activity, the Bot User conducted a series of transactions to conceal or disguise the nature, location, source, ownership, or control of the proceeds.

59. On April 28, 2023, the Bot User sent the funds from 0x237D in three transactions of 10 BNB, 5466 BNB, and 0.12 BNB to 0x0D5c28F489229b5A58be8208142d9199ea1250c6 (“0x0D5x”).

60. On the same day, the funds were sent from 0x0D5x to another virtual address, 0x9C48dBaedE745D02B32632127a7C281920ee6055 (“0x9C48”).

61. Between April 28, 2023, and May 1, 2023, 0x9C48 sent the approximately 5,476 BNB to virtual address 0x73c5e6f1573ce8ceac6fb83bf0fec162a77ddf42e (“0x73c5”), an address associated with an account at the crypto exchange, Matrixport.

62. Those funds were then withdrawn from the account containing 0x73c5 and sent in nineteen transactions to 7 different virtual addresses, which are attributed to 2 accounts at OKX and 1 account at China-based crypto company, Huobi. The funds in these transactions can be seen coming directly from 0x73c5 or other Matrixport addresses due to an internal transfer settlement process in which any withdrawal requests will extract available funds from potentially all hot wallets maintained on the Matrixport Platform, including wallet addresses not assigned to a specific user.

63. The funds involved in this series of transactions, as explained above, were the proceeds of: (i) wire fraud, in violation of 18 U.S.C. § 1343; (ii) the use of a facility in interstate or foreign commerce in aid of racketeering enterprises, in violation of 18 U.S.C. §§ 1952(a)(1)(A) & 1952(a)(3)(A); and (iii) fraud in connection with computers, in violation of 18 U.S.C. § 1030.

64. On May 2, 2023, pursuant to a request by the Federal Bureau of Investigation ("FBI"), the crypto company OKX identified two accounts that contained funds transferred from the account holder of 0x73c5.

65. On May 3, 2023, OKX froze the funds contained in those accounts.

66. The first account, identified by the unique ID 422338420543782467 ("OKX Account 1"), contained the equivalent of approximately 2,003 BNB deposited from the account holder of 0x73c5.

a. There were eight total deposit transactions made to OKX Account 1 from the account holder of 0x73c5 on April 28, 2003.

b. On that day, BNB was deposited into OKX Account 1 in the individual amounts of 20, 82, 201, 700, 307, 307, 307, and 79, for a total of 2,003 BNB.

c. On the same day, the value of the account funds was converted to Tether tokens ("USDT"), another blockchain-based cryptocurrency, in the amount of 681,418.24 USDT.

67. The second account, identified by the unique ID 438957971071216816 ("OKX Account 2"), contained approximately 481 BNB deposited from the account holder of 0x73c5.

a. There were seven total deposit transactions made to OKX Account 2 from the account holder of 0x73c5 on May 1, 2023.

b. On that day, BNB was deposited into this account in the individual amounts of 20, 20, 20, 20, 200, 100, and 101 for a total of 481 BNB.

68. The 15 deposits into these two OKX accounts represent approximately half of the 20% of the proceeds that the Bot User unlawfully obtained.

69. The remaining funds that the Bot User transferred from the account holder of 0x735c were transferred to a China-based crypto company, Huobi.

70. The Bot User designed and conducted these transactions in whole or in part to disguise the nature, location, source, ownership, or control of the funds.

71. Ultimately, the FBI obtained a lawful seizure warrant for the contents of OKX Account 1 and OKX Account 2 on May 15, 2023, and an amended warrant was obtained on May 23, 2023.

72. The FBI successfully seized 680,467.92 USDT from OKX Account 1 and 480.996 BNB from OKX Account 2.

COUNT 1
(Forfeiture Under 18 U.S.C. § 981(a)(1)(C)
as Proceeds of Wire Fraud in Violation of 18 U.S.C. § 1343)

73. The United States incorporates by reference Paragraphs 1 through 72 of this Complaint as if fully set forth herein.

74. Title 18, United States Code, Section 981(a)(1)(C) subjects to forfeiture "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting 'specified unlawful activity' (as defined in section 1956(c)(7) of this title) or a conspiracy to commit such an offense."

75. Title 18, United States Code, Section 1956(c)(7)(D) provides that the term "specified unlawful activity" includes "an offense under . . . section 1343 (relating to wire fraud)."

76. As set forth above, the Defendant Property constitutes criminal proceeds of wire fraud.

77. As such, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

COUNT 2
(Forfeiture Under 18 U.S.C. § 981(a)(1)(A)
as Property Involved in a Transaction in Violation of 18 U.S.C. § 1956)

78. The United States incorporates by reference Paragraphs 1 through 72 of this Complaint as if fully set forth herein.

79. Title 18, United States Code, Section 981(a)(1)(A) subjects to forfeiture "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956 . . . of this title, or any property traceable to such property."

80. Title 18, United States Code, Section 1956(a)(1)(B)(i) imposes criminal liability on "[w]hoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity . . . knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity."

81. As set forth above, the Defendant Property constitutes property involved in a violation of section 1956.

82. As such, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

COUNT 3
(Forfeiture under 18 U.S.C. § 981(a)(1)(C)
as Proceeds of Unlawful Activity Under 18 U.S.C. § 1952)

83. The United States incorporates by reference Paragraphs 1 through 72 of this Complaint as if fully set forth herein.

84. Title 18, United States Code, Section 981(a)(1)(C) subjects to forfeiture "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting 'specified unlawful activity' (as defined in section 1956(c)(7) of this title) or a conspiracy to commit such an offense."

85. Title 18, United States Code, Section 1956(c)(7)(A) provides that the term "specified unlawful activity" includes "any act or activity constituting an offense listed in section 1961(1) of this title."

86. Among other offenses, Title 18, United States Code, Section 1961(1), lists "any act which is indictable under . . . section 1952 (related to racketeering)."

87. Title 18, United States Code, Section 1952, in turn, establishes criminal liability for the use of "any facility in interstate or foreign commerce, with intent to distribute the proceeds of any unlawful activity; or . . . promote, manage, establish, carry on . . . any unlawful activity."

88. Section 1952 defines the term "unlawful activity" to include "extortion . . . in violation of the laws of the State in which committed."

89. Virginia Code § 18.2-59 provides that "[a]ny person who . . . threatens injury to the character, person, or property of another person . . . and thereby extorts money, property, or pecuniary benefit . . . from him or any other person, is guilty of a felony."

90. Similarly, section 76-6-406 of the Utah Criminal Code provides, in relevant part, that "[a]n actor commits theft by extortion if the actor obtains or exercises control over the property of another person by extortion and with a purpose to deprive the person of the person's property," and a violation of this section constitutes a second degree felony where the value of the property exceeds $5,000.

91. As set forth above, the defendant property constitutes criminal proceeds of a violation of 18 U.S.C. § 1952.

92. As such, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

COUNT 4
(Forfeiture Under 18 U.S.C. § 981(a)(1)(C) as Proceeds of Computer Fraud in Violation of 18 U.S.C. § 1030(a)(4))

93. The United States incorporates by reference Paragraphs 1 through 72 of this Complaint as if fully set forth herein.

94. Title 18, United States Code, Section 981(a)(1)(C) subjects to forfeiture "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to a violation of section…1030…of this title…or a conspiracy to commit such offense."

95. Relevant here, Title 18, United States Code, Section 1030(a)(4) imposes criminal liability on "whoever . . . knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value."

96. As set forth above, the Defendant Property constitutes criminal proceeds of a violation of 18 U.S.C. § 1030(a)(4).

97. As such, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

PRAYER FOR RELIEF

WHEREFORE, the United States requests that judgment be entered in its favor against the Defendant Property; that pursuant to law, notice be provided to all interested parties to appear and show cause why the forfeiture should not be decreed; that the Defendant Property be forfeited to the United States and delivered into its custody for disposition according to law; that the United States be awarded its costs and disbursements in this action; and for such and further relief as this Court may deem just and proper.

Dated: June 18, 2024

Respectfully submitted,

JESSICA D. ABER
UNITED STATES ATTORNEY

By: /s/ Kevin Hudson
Kevin Hudson
Assistant United States Attorney
Virginia State Bar No. 81420
Attorney for the United States
11815 Fountain Way, Suite 200
Newport News, VA 23606
Office Number: (757) 591-4000
Facsimile Number: (757) 591-0866
Email Address: kevin.hudson@usdoj.gov

VERIFICATION

I, Cindi A. Zealor, Special Agent, Federal Bureau of Investigation, declare under penalty of perjury as provided by 28 U.S.C. § 1746, that the foregoing Complaint for Forfeiture *in Rem* is based on information known by me personally and/or furnished to me by various federal, state, and local law enforcement agencies, and that everything contained herein is true and correct to the best of my knowledge.

Executed at Alexandria Virginia, this 5th of June, 2024.

Cindi Zealor
Cindi A. Zealor
Special Agent
Federal Bureau of Investigation